

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-240826

(43)Date of publication of application : 11.09.1998

(51)Int.Cl.

G06F 17/60

G09C 1/00

H04L 9/08

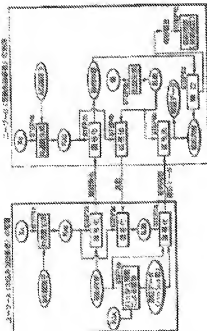
(21)Application number : 09-047962

(71)Applicant : CARD KOOLE SERVICE KK

(22)Date of filing : 03.03.1997

(72)Inventor : BABA YOSHIMI

(54) ELECTRONIC CONTRACTING METHOD

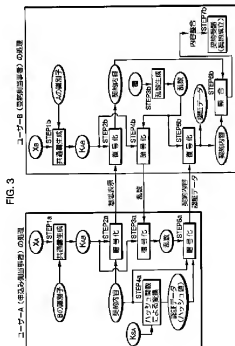


(57)Abstract:

PROBLEM TO BE SOLVED: To provide an electronic contracting method for constructing a simple and prevailing electronic contracting system in which cipher communication using a common key can be operated, and the reliability of contract can be improved between persons concerned.

SOLUTION: When a user B receives the indication of the intention of the conclusion of contract from a user A, the user B generates a random number using one generative number as a seed by its own terminal equipment, enciphers it by a common key K_{AB} with the user A, and transmits it to the user A. The user A decodes the random number by the common K_{AB}, enciphers a contract content by using the random number as a key, transmits it to the user B, and applies for contract to the user B. Moreover, the user A transmits certification data

obtained by converting the contract content by a hash function decided by its own secret key K_{SA} to the user B.



【特許請求の範囲】

【請求項1】ネットワーク上の二人の当事者の一方を契約の申込み側、他方を該契約の受諾側として、両当事者がそれぞれ所持する端末装置間をオンライン通信により前記契約を行う電子契約方法において、

各当事者の端末装置に、あらかじめ前記契約を行う相手側の当事者の識別子を入力することにより両当事者間での有効な暗号通信用の共通鍵を生成する手段と、通信データの暗号・復号化を行う手段とを具備しておき、

前記受諾側当事者は、前記申込み側当事者から前記契約の締結の意思表示を受けたとき、該受諾側当事者の端末装置により、前記申込み側当事者の識別子を入力して該申込み側当事者との前記共通鍵を生成した後、前記申込み側当事者には不知で該受諾側当事者に固有の受諾側固有データを前記共通鍵を用いて暗号化して前記申込み側当事者の端末装置に送信し、

その暗号化された前記受諾側固有データを受信した前記申込み側当事者は、該申込み側当事者の端末装置により、前記受諾側当事者の識別子を入力して該受諾側当事者との前記共通鍵を生成した後、その共通鍵を用いて前記暗号化された受諾側固有データを復号し、さらに、前記受諾側当事者と契約しようとする契約内容を、前記復号化した受諾側固有データを鍵として用いて暗号化した後、その暗号化した契約内容を前記受諾側当事者の端末装置に送信することにより前記受諾側当事者に前記契約を申込み、

前記受諾側固有データを鍵として暗号化された前記契約内容を受信した前記受諾側当事者は、該受諾側当事者の端末装置により、前記暗号化された契約内容を該受諾側当事者の前記受諾側固有データを鍵として用いて復号し、その復号化した前記契約内容に基づき、前記契約を受諾することを特徴とする電子契約方法。

【請求項2】前記受諾側当事者は、前記受諾側固有データを暗号化して前記申込み側当事者に送信する前に、該受諾側当事者の端末装置により、一回性の数値として該種が逆算不能な乱数を生成し、その生成した乱数を前記受諾側固有データとして用いることを特徴とする請求項1記載の電子契約方法。

【請求項3】前記乱数の種となる前記一回性の数は、前記受諾側当事者の端末装置における人為的入力操作の時間的タイミングに基づき生成することを特徴とする請求項2記載の電子契約方法。

【請求項4】前記申込み側当事者は、前記受諾側当事者に前記契約の締結の意思表示をするとき、前記契約内容又はその概要を示す予備契約内容を、前記受諾側当事者との前記共通鍵を用いて該申込み側当事者の端末装置により暗号化して前記受諾側当事者の端末装置に送信し、前記受諾側当事者は、前記契約を受諾する際に、前記共通鍵を用いて暗号化された前記契約内容又は予備契約内容を該受諾側当事者の端末装置により復号化したもの

と、前記受諾側固有データを鍵として暗号化された前記契約内容を該受諾側当事者の端末装置により復号化したものと照合して、該契約内容を確認することを特徴とする請求項1乃至3のいずれかに記載の電子契約方法。

【請求項5】前記申込み側は、前記契約を前記受諾側当事者に申し込む際に、該申込み側当事者の端末装置により、少なくとも前記契約内容に、該申込み側当事者及び前記受諾側当事者以外の公証能力を有する第三者が認証可能な該申込み側当事者に固有の秘密鍵に基づき加工を施して該契約内容に固有で且つ申込み側当事者に固有の認証データを生成し、その生成した認証データを前記受諾側当事者に送信することを特徴とする請求項1乃至4のいずれかに記載の電子契約方法。

【請求項6】前記認証データは、前記契約内容のデータもしくは該契約内容を前記受諾側固有データを鍵として暗号化してなるデータ、又はこれらのデータに契約の申込みの日にちに応じたデータを付加してなるデータを、前記秘密鍵により定まる一方向性関数により変換することにより生成することを特徴とする請求項5記載の電子契約方法。

【請求項7】前記契約の申込みの日にちに応じたデータは、該日時を示す数値を前記一方向性関数又は統一方向性関数とは異なる一方向性関数により変換してなるデータであることを特徴とする請求項6記載の電子契約方法。

【請求項8】前記認証データは、前記契約内容のデータもしくは該契約内容を前記受諾側固有データを鍵として暗号化してなるデータ、又はこれらのデータに契約の申込みの日にちに応じたデータを付加してなるデータを、所定の一方性関数により変換した後、その変換データを前記秘密鍵により暗号化することにより生成することを特徴とする請求項5記載の電子契約方法。

【請求項9】前記契約の申込みの日にちに応じたデータは、該日時を示す数値を前記一方向性関数又は統一方向性関数とは異なる一方向性関数により変換してなるデータであることを特徴とする請求項8記載の電子契約方法。

【請求項10】前記申込み側当事者は、前記契約を前記受諾側当事者に申し込む際に、前記一方向性関数により得られた前記変換データを前記受諾側当事者の端末装置に送信し、

該変換データを受信した前記受諾側当事者は、該受諾側当事者の端末装置により、前記受諾側固有データを鍵として復号化した前記契約内容を、前記申込み側当事者の一方向性関数と同一の一方向性関数により変換し、さらに、前記契約を受諾する際に、前記受諾側当事者の端末装置から送信されてきた前記変換データと、前記受諾側固有データを鍵として復号化した前記契約内容を前記申込み側当事者の一方向性関数と同一の一方向性関数により変換してなるデータとを照合して前記変換データを確

認することを特徴とする請求項8又は9記載の電子契約方法。

【請求項11】前記申込み側当事者は、前記変換データを、該申込み側当事者の端末装置により前記受諾側固有データを鍵として暗号化して前記受諾側当事者の端末装置に送信し、前記受諾側当事者は、その暗号化された変換データを該受諾側当事者の端末装置により前記受諾側固有データを鍵として復号化することを特徴とする請求項10記載の電子契約方法。

【請求項12】前記申込み側当事者は、前記認証データを、該申込み側当事者の端末装置により前記受諾側固有データを鍵として暗号化して前記受諾側当事者の端末装置に送信し、前記受諾側当事者は、その暗号化された認証データを該受諾側当事者の端末装置により前記受諾側固有データを鍵として復号化することを特徴とする請求項5乃至11のいずれかに記載の電子契約方法。

【請求項13】前記契約の締結後に、前記申込み側当事者及び受諾側当事者は、少なくとも前記契約内容と前記受諾側固有データと前記変換データと前記認証データとを前記第三者に送って保管せしめることを特徴とする請求項1乃至12のいずれかに記載の電子契約方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、インターネット、パソコン通信網等のネットワークを用いたオンライン通信によって、商品の売買やそれに伴う課金、決済等を含む、各種の契約を行う電子契約方法に関する。

【0002】

【従来の技術】ネットワーク上の二人の当事者間で、その一方を契約の申込み側、他方を契約の受諾側としてオンライン通信によって各種の契約を結ぶ場合、その契約を安全に行い、該契約の信頼性を高めるためには、契約内容を第3者が偽造できない（third party condition

以下、条件Tという）、契約内容を受信者（契約の受諾者）が偽造できない（Receiver condition、以下、条件Rという）、契約内容を送信者（契約の申込み者）が事後否定できない（Sender condition、以下、条件Sという）というような条件が満たされることが必要であると一般に言われている（例えばW.Diffie及びM.E.Hellmanによる論文「New directions in cryptography」/IEEE, IT, vol.IT-22, No.6, pp.644-654, 1976.11.」を参照）。特に、商品の売買契約等においては、前記条件Sが不十分であると、後々の当事者間の争いの元となることが多く、この条件Sを可能な限り満たすことが望ましい。

【0003】ところで、従来の電子契約の手法としては、例えばは契約の申込み者に固有のパスワードを利用したものが一般に普及している。

【0004】この手法では、例えばネットワーク上の契約の申込み側当事者としてあるユーザが、契約の受諾

側当事者としての商品販売者から商品を購入する契約を結ぼうとするとき、該ユーザはあらかじめ商品販売者に登録した該ユーザの固有のパスワードを使用して該商品販売者に商品購入の申込みをオンライン通信で行う。そして、その申込みの通信を受けた商品販売者は、上記パスワードに基づきユーザを認証して、該ユーザによる商品購入やその代金支払いの申込みを受諾し、その受諾した内容に従って商品をユーザに受け渡したり、代金請求を行ったりする。

【0005】しかるに、この手法では、ユーザと商品販売者との間で契約内容やパスワードがそのまま通信されるため、パスワードが第三者に盗用されたり、契約内容が第三者により偽造されたりする危険性が高い。このため、例えば前記条件Tを満たすことが難しく、信頼性の高い契約を行うことが困難である。

【0006】また、近年では、所謂、RSA暗号を用いた公開鍵方式による電子契約の手法も知られている。

【0007】この手法では、例えば前記のような商品購入の契約を行うとき、ユーザは、商品購入の申込み内容を、ネットワーク上の鍵管理局から与えられた該ユーザに固有の秘密鍵を用いて暗号化し、それを商品販売者に送信する。また、その暗号化された申込みを受けた商品販売者側では、鍵管理局が公開しているユーザの公開鍵を参照し、その公開鍵を用いて暗号化された申込み内容を復号化する。そして、この復号化した申込み内容に基づき、ユーザによる商品購入やその代金支払いの申込みを受諾する。この場合、ユーザの公開鍵を用いて正常に復号化することができるのは、該ユーザの秘密鍵を用いて暗号化されたものだけであるので、商品販売者はユーザから受けた申込み内容が正常に復号化されるか否かによって、ユーザを認証することができる。

【0008】このような公開鍵方式による手法では、契約の当事者間の通信は暗号によって行われるため、その通信内容の秘密性が確保され、第三者による契約内容の偽造等が困難である。また、契約の申込み側当事者であるユーザの公開鍵によって復号化できる暗号文は該ユーザの秘密鍵によって暗号化されたものに限定するため、ユーザが契約事実を事後否定したり、契約の受諾側当事者である商品販売者が契約内容を偽造することも困難となる。従って、前記条件T、R、Sを満たし易く、契約の信頼性を高めることができる。

【0009】しかるに、この公開鍵方式では、一般にその暗号通信のためのデータ処理量が大きなものとなって非効率なものとなり易く、また、通信に際して、その都度、公開鍵の参照等のために鍵管理局と通信を行ったりしなければならず、手間のかかるものとなっていた。さらに、鍵管理局では、公開鍵を厳格に保守・管理しなければならぬため、該鍵管理局の負担が大きく、多数のユーザがシステムに加入することが困難である。従って、このような公開鍵方式による手法では、簡易で普及

性の高い電子契約システムを構築することが困難なものとなっていた。

【0010】一方、暗号通信においては、前記公開鍵方式のように暗号化と復号化とで異なる鍵を使用する非対称型の暗号通信方式の他、暗号化と復号化とで同じ鍵を使用する対称型の暗号通信方式が知られている。そして、このような対称型の暗号通信方式としては、例えば Rolf Blom による論文「NON-BLIND KEY DISTRIBUTION / Advances in Cryptology: Proceedings of CRYPTO '82 / Plenum Press 1983, pp.231-236」、同じく Rolf Blom による論文「An Optimal Class of Symmetric Key Generation Systems / Advances in Cryptology: EUROCRYPT '84 / Springer LNCS 209, 1985, pp.335-338」、あるいは特公平5-48980号公報もしくは米国特許第5016278号に見られるように、あらかじめ鍵管理局から各ユーザに、該ユーザ固有の個人鍵（アルゴリズム）を配付しておき、通信に際しては、各ユーザが自己の個人鍵に通信相手側の名前等の公開性の識別子を入力することで、その通信相手側の暗号通信を行うための共通鍵を生成することができるようにしたもの知られる。

【0011】このような暗号通信方式によれば、各ユーザは、暗号通信を行う際には、鍵管理局との事前通信等を行うことなく、自己の個人鍵に通信相手側の名前等の公開性の識別子を入力するだけで、随時、通信相手側との暗号通信用の共通鍵を生成することができ、また、鍵管理局は、各ユーザの個人鍵を発行すればよいだけなので、その負担も小さい。

【0012】従って、このような共通鍵による暗号通信方式を電子契約に適用できれば、簡易で普及性の高い電子契約システムを提供することができると考えられる。

【0013】しかしながら、このような共通鍵による暗号通信方式を用いてオンライン通信による契約を行おうとした場合、その契約の両当事者が、いつでも随に、相手側との共通鍵を生成できるため、単に、契約内容を共通鍵により暗号化して両当事者間で授受しただけでは、契約の信頼性を充分に確保することが困難である。

【0014】すなわち、二者間で契約を締結する場合、その契約の信頼性を高める上で、前記条件T、R、Sが満たされること一つの特徴として重要ではあるが、その他、書面による通常の契約の場合における各当事者の署名や捺印等、各当事者にしかなく、より好ましくは、当事者以外の者が公的に認証し得るものを相手側の当事者に与えることが重要である。さらに、前述のように、共通鍵を用いた暗号通信により契約を結ぼうとした場合、該共通鍵は、両当事者が随時生成することができるものであるため、単に、契約内容を共通鍵により暗号化して両当事者間で授受しただけでは、各当事者は互いに相手側に各当事者しかなく得ないものを与えることができず、契約の信頼性を充分に確保することが困

難である。

【0015】

【発明が解決しようとする課題】本発明はかかる背景に鑑み、契約の当事者間で、共通の鍵を使用した暗号通信を行いつつ契約の信頼性を高めることができると共に、簡易で普及性の高い電子契約システムを構築することができる電子契約方法を提供することを目的とする。

【0016】

【課題を解決するための手段】本発明の電子契約システムはかかる目的を達成するために、ネットワーク上の二人の当事者の一方を契約の申込み側、他方を該契約の受諾側として、両当事者がそれぞれ所持する端末装置間のオンライン通信により前記契約を行う電子契約方法において、各当事者の端末装置に、あらかじめ前記契約を行う相手側の当事者の識別子を入力することにより両当事者間でのみ有効な暗号通信用の共通鍵を生成する手段と、通信データの暗号・復号化を行う手段とを備えておき、前記受諾側当事者は、前記申込み側当事者から前記契約の締結の意思表示を受けたとき、該受諾側当事者の端末装置により、前記申込み側当事者の識別子を入力して該申込み側当事者との前記共通鍵を生成した後、前記申込み側当事者には不知で該受諾側当事者に固有の受諾側固有データを前記共通鍵を用いて暗号化して前記申込み側当事者の端末装置に送信し、その暗号化された前記受諾側固有データを受信した前記申込み側当事者は、該申込み側当事者の端末装置により、前記受諾側固有データの識別子を入力して該受諾側当事者との前記共通鍵を生成した後、その共通鍵を用いて前記暗号化された前記受諾側固有データを復号化し、さらに、前記受諾側当事者と契約しようとする契約内容を、前記復号化された受諾側固有データを鍵として用いて暗号化した後、その暗号化した契約内容を前記受諾側当事者の端末装置に送信することにより前記受諾側当事者に前記契約の申込み、前記受諾側固有データを鍵として暗号化された前記受諾側内容を受信した前記受諾側当事者は、該受諾側当事者の端末装置により、前記暗号化された契約内容を該受諾側当事者の前記受諾側固有データを鍵として用いて復号化し、その復号化した前記契約内容に基づき、前記契約を遂行することを特徴とする。

【0017】かかる本発明によれば、前記受諾側当事者は、前記申込み側当事者から契約の締結の申込みを受けたとき、該受諾側当事者に固有で且つ申込み側当事者には不知の前記受諾側固有データを、申込み側当事者との前記共通鍵を用いて暗号化して、申込み側当事者の端末装置に送信する。この場合、申込み側当事者との共通鍵は、受諾側当事者の端末装置に該受諾側当事者の通信相手である申込み側当事者の識別子を入力することによって生成される。

【0018】一方、上記のように暗号化された前記受諾側固有データを自身の端末装置で受信した前記申込み側

当事者は、その略号化された受諾側固有データを受諾側当事者との前記共通鍵を用いて復号化する。この場合、受諾側当事者との共通鍵は、申込み側当事者の端末装置に受諾側当事者の氏名等の識別子を入力することで生成される。

【0019】尚、各当事者が前述の如く通信相手側との共通鍵を生成するために必要な各当事者の識別子は、各当事者の氏名、住所、ネットワーク上のメールアドレス、ドメイン名、あるいはそれらを組み合わせたもの等、各当事者に固有で且つ公開性のあるものを使用する。

【0020】次に、上記のように受諾側固有データを復号化した申込み側当事者は、その受諾側固有データを鍵として、前記契約内容を略号化して受諾側当事者の端末装置に送信し、これにより前記契約を受諾側当事者に申し込む。そして、このように受諾側固有データを鍵として略号化された前記契約内容を自身の端末装置で受信した受諾側当事者は、自身が所持する前記受諾側固有データを鍵として、該契約内容を復号化し、その復号化した契約内容に基づき申込み側当事者との契約を受諾する。

【0021】このような契約を行う本発明の電子契約方法によれば、申込み側当事者は、受諾側当事者に固有で、しかも該申し込み側当事者が事前には知り得ない受諾側固有データを鍵として契約内容を略号化して、受諾側当事者に契約を申し込むので、受諾側当事者は、自身が独自に指定した独特な方式で申込み側当事者からの契約の申込みを受けることとなる。このため、該受諾側当事者にとっては、申込み側当事者による契約の申込みの信頼性が高まる。同時に、申込み側当事者は、受諾側当事者が独自に指定した方式に従って契約を申し込むこととなるため、契約の事後否定をしにくくなる。また、受諾側当事者から申込み側当事者への前記受諾側固有データの略号通信のための前記共通鍵は、両当事者がそれぞれ各別に自身の端末装置に相手側の識別子を入力するだけで両当事者が共有することができ、さらに、申込み側当事者から受諾側当事者への前記契約内容の略号通信のための鍵は、その鍵として前記受諾側固有データを受諾側当事者から申込み側当事者に前記共通鍵により略号化して与えるだけで、両当事者が共有することができるので、提管管理局等の第三者の関与を伴うことなく、両当事者だけで、支障なく契約のための通信を行うことができる。さらには、両当事者間の通信は略号通信によって行われるので、その通信データ（受諾側固有データ及び契約内容）の部外者に対する機密性が保たれる。

【0022】従って、本発明によれば、契約の当事者間で、共通の鍵を使用した略号通信を行いつつ契約の信頼性を高めることができると共に、簡易で普及性の高い電子契約システムを構築することができる。

【0023】かかる本発明では、前記受諾側当事者は、前記受諾側固有データを略号化して前記申込み側当事者

に送信する前に、該受諾側当事者の端末装置により、一回性の数を種として該種が逆算不能な乱数を生成し、その生成した乱数を前記受諾側固有データとして用いることが好ましい。ここで、前記一回性の数は、再現性がなく、もしくは再現性に極めて乏しい数である。

【0024】このように受諾側当事者の端末装置で一回性の数を種として生成した乱数を前記受諾側固有データとして用いることで、受諾側当事者における該受諾側固有データの独自性が強まり、このような受諾側固有データを鍵として、前記申込み側当事者から前記契約内容を略号化して受諾側当事者に送信することで、その契約内容に基づく、両当事者間の契約の信頼性が効果的に高まる。

【0025】この場合、前記乱数の種となる前記一回性の数は、例えば前記受諾側当事者の端末装置における人為的入力操作の時間的タイミングに基づき生成する。このように、受諾側当事者の端末装置における人為的入力操作（例えばある文章や語句を入力する操作）の時間的タイミングに基づき生成される数は、人間による操作のあいまいさによって、偶然的な予想のつかないものとなる。従って、再現性がなく、もしくは再現性に極めて乏しい一回性の数を的確に生成することができ、その数を種として生成した乱数を受諾側固有データとして使用することで、該受諾側固有データの独自性を良好に確保することができる。

【0026】また、本発明では、前記申込み側当事者は、前記受諾側当事者に前記契約の締結の意思表示をするとき、前記契約内容又はその概要を示す予備契約内容を、前記受諾側当事者との前記共通鍵を用いて該申込み側当事者の端末装置により略号化して前記受諾側当事者の端末装置に送信し、前記受諾側当事者は、前記契約を受諾する際に、前記共通鍵を用いて略号化された前記契約内容又は予備契約内容を該受諾側当事者の端末装置により復号化したものと、前記受諾側固有データを鍵として略号化された前記契約内容を該受諾側当事者の端末装置により復号化したものとを照合して、該契約内容を確認する。

【0027】このように、申込み側当事者が、受諾側当事者に契約の締結の意思表示を行う際に、前記共通鍵を用いた略号通信によって、前記契約内容又はその概要を示す予備契約内容を受諾側当事者に与えておくことで、受諾側当事者は、最終的に契約を承諾するに際して、前記共通鍵を用いて略号化された前記契約内容又は予備契約内容を復号化したものと、前記受諾側固有データを鍵として略号化された前記契約内容を復号化したものとを照合して、それらの整合性を確認した上で、契約を承諾することができる。また、該受諾側当事者にとって、申込み側当事者との契約の信頼性をより一層高めることができる。

【0028】さらに、本発明では、前記申込み側は、前記契約を前記受諾側当事者に申し込む際に、該申込み側

当事者の端末装置により、少なくとも前記契約内容に、該申込み側当事者及び前記受諾側当事者以外の公証能力を有する第三者が認証可能な該申込み側当事者に固有の秘密鍵に基づく加工を施して該契約内容に固有で且つ申込み側当事者に固有の認証データを生成し、その生成した認証データを前記受諾側当事者に送信する。

【0029】このように、前記申込み側当事者が受諾側当事者に契約を申し込む際に、前記契約内容に、前記申込み側当事者に固有で且つ前記第三者が認証可能な秘密鍵に基づく加工を施して、該契約内容に固有で且つ申込み側当事者に固有の認証データを生成し、それを受諾側当事者に送信することで、受諾側当事者には、前記契約内容に申込み側当事者が公的な署名もしくは捺印を施したものに相当する認証データが申込み側当事者から与えられることとなる。これにより、両当事者にとって、契約の信頼性がより強固なものとなる。

【0030】この場合、前記認証データは、前記契約内容のデータもしくは該契約内容を前記受諾側固有データを鍵として暗号化してなるデータ、又はこれらのデータに契約の申込みの日時に応じたデータを付加してなるデータを、前記秘密鍵により定まる一方方向性関数により変換する。

【0031】あるいは、前記認証データは、前記契約内容のデータもしくは該契約内容を前記受諾側固有データを鍵として暗号化してなるデータ、又はこれらのデータに契約の申込みの日時に応じたデータを付加してなるデータを、所定の一方方向性関数により変換した後、その変換データを前記秘密鍵により暗号化することにより生成する。

【0032】これによれば、前記契約内容もしくはこれを前記受諾側固有データを鍵として暗号化したもの、又はこれらに契約の日時に応じたデータを付加したもの（以下、ここでは契約内容等と称する）と申込み側当事者とに固有の認証データを正確に生成することができる。また、認証データの生成に際して、契約内容等を一方方向性関数を用いて変換するので、生成した認証データを受諾側当事者に与えた後に、例えば申込み側当事者が契約内容を改ざんしようとしても、該申込み側当事者は、受諾側当事者に与えた認証データと整合するように契約内容を改ざんすることは難しく、申込み側当事者が契約内容を事後否定することは困難なものとなる。また、前記認証データは、申込み側当事者の秘密鍵に基づいて生成されるので、例えば該申込み側当事者が、受け取った認証データに整合するように契約内容を改ざんすることも困難である。従って、前記契約の信頼性を両当事者間で効果的に高めることができる。

【0033】尚、前記契約の申込みの日時に応じたデータを付加する場合、前記契約の申込みの日時に応じたデータは、該日時を示す数値を前記一方方向性関数又は該一方方向性関数とは異なる一方方向性関数により変換してなる

データであることが好ましい。このように契約の日時を一方方向性関数により変換しておくことで、後に、契約の申込みの日時を改ざんしようとしても、その改ざんが困難なものとなる。

【0034】前述のように前記契約内容等を所定の一方方向性関数により変換した後、その変換データを前記秘密鍵を鍵として暗号化する場合、前記申込み側当事者は、前記契約を前記受諾側当事者に申し込む際に、前記一方方向性関数により得られた前記変換データを前記受諾側当事者の端末装置に送信し、該変換データを受信した前記受諾側当事者は、該受諾側当事者の端末装置により、前記受諾側固有データを鍵として復号化した前記契約内容を、前記申込み側当事者の一方方向性関数と同一の一方方向性関数により変換し、さらに、前記契約を受諾する際に、前記受諾側固有データの端末装置から送信された前記変換データと、前記受諾側固有データを鍵として復号化した前記契約内容を前記申込み側当事者の一方方向性関数と同一の一方方向性関数により変換してなるデータとを照合して前記変換データを確認することが好ましい。

【0035】このように前記契約内容等を申込み側当事者が所定の一方方向性関数により変換して成る変換データを受諾側当事者に送信し、また、受諾側当事者においては、前記受諾側固有データを鍵として復号化した前記契約内容を申込み側当事者と同一の一方方向性関数によって変換してなるデータと、前記受諾側当事者から送られてきた変換データとを照合することで、前記変換データが正式な契約内容（受諾側固有データを鍵として復号化した契約内容）に基づいて生成されたものであるかを確認することができる。これにより、契約の信頼性をさらに高めることができる。

【0036】尚、前記変換データの通信においては、前記申込み側当事者は、前記変換データを、該申込み側当事者の端末装置により前記受諾側固有データを鍵として暗号化して前記受諾側当事者の端末装置に送信し、前記受諾側当事者は、その暗号化された変換データを該受諾側当事者の端末装置により前記受諾側固有データを鍵として復号化することが好ましい。

【0037】また、前記認証データの通信においては、前記申込み側当事者は、前記認証データを、該申込み側当事者の端末装置により前記受諾側固有データを鍵として暗号化して前記受諾側当事者の端末装置に送信し、前記受諾側当事者は、その暗号化された認証データを該受諾側当事者の端末装置により前記受諾側固有データを鍵として復号化することが好ましい。

【0038】このように契約の信頼性を高める上で重要な前記変換データや認証データを暗号化して通信することで、該変換データや認証データの部外者に対する機密性を確実に確保することができる。

【0039】また、契約に際して、前記認証データや変換データを通信する場合、前記契約の締結後に、前記申

込み側当事者及び受諾側当事者は、少なくとも前記契約内容と前記受諾側固有データと前記変換データと前記認証データとを前記第三者に送って保管せしめることが特に好適である。

【0040】このように、各当事者が前記契約内容や前記受諾側固有データ、前記変換データ、前記認証データをこれらの当事者から中立的な第三者に送って保管せしめることで、契約の効力を確実なものとなることができ

る。

【0041】
【発明の実施の形態】本発明の第1の実施形態を図1乃至図3を参照して説明する。図1は本実施形態の電子契約方法を適用した電子契約システムの全体的構成を示す説明図、図2は本実施形態において契約を行う当事者が所持する端末装置の機能的構成を示すブロック図、図3は本実施形態で契約を行う際の処理手順を示すフロー図である。

【0042】図1を参照して、本システムでは、複数のユーザーA、B、…がそれぞれ所持する端末装置1a、1b、…と、暗号通信用の鍵の発行等を担う鍵管理局Cの端末装置2と、暗号通信用の鍵の認証等を行う公証人Sの端末装置3とがインターネット、パソコン通信網等のネットワーク4を介して相互に通信可能に接続されている。各端末装置1a、1b、…、2、3は、パソコン等のコンピュータマシンと通信機器、あるいはそれに付帯したソフトウェア等により構成されている。この場合、各ユーザーA、B、…には、他の任意のユーザーとの間で暗号通信用の共通鍵を生成するための各ユーザーA、B、…に固有の共通鍵生成用アルゴリズム X_A 、 X_B 、…があらかじめ鍵管理局Cから配付され、公証人Sとの間で暗号通信用の共通鍵 K_{AS} 、…が各ユーザーA、B、…に固有の秘密鍵としてあらかじめ鍵管理局Cから配付されている。それらの共通鍵生成用アルゴリズム X_A 、 X_B 、…や秘密鍵 K_{AS} 、 K_{BS} 、…は、それぞれ各ユーザーA、B、…の端末装置1a、1b、…（以下、必要に応じて端末装置1と総称する）に保管されている。

【0043】また、前記公証人Sには、任意のユーザーA、B、…との間で暗号通信用の共通鍵 K_{AS} 、 K_{BS} 、…（＝各ユーザーA、B、…の秘密鍵）を生成するための公証人Sに固有の共通鍵生成用アルゴリズム X_S があらかじめ鍵管理局Cから配付され、それが公証人Sの端末装置3に保管されている。これにより、公証人Sは、必要に応じて、自身の共通鍵生成用アルゴリズム X_S を用いて、各ユーザーA、B、…との共通鍵 K_{AS} 、 K_{BS} 、…を生成し、それを各ユーザーA、B、…が所持する秘密鍵 K_{AS} 、 K_{BS} 、…と照合することで、各ユーザーA、B、…の秘密鍵 K_{AS} 、 K_{BS} 、…を認証することができるようにしている。

【0044】ここで、各ユーザーA、B、…や公証人S

が所持する共通鍵生成用アルゴリズム X_A 、 X_B 、…、 X_S は、前述のRoIt Blomの論文や特公平5-48980号公報、米国特許第5016276号に見られるもののように、通信相手側の名前、住所等、その通信相手に固有で公開性のある識別子を入力することでその通信相手側との暗号通信用の共通鍵を生成するものである。

【0045】図2に示すように、各ユーザーA、B、…の端末装置1には、そのハードウェアやソフトウェアによる機能的構成として、乱数を生成する乱数生成手段5と、前述の如く通信相手側の識別子を入力することで前記共通鍵生成用アルゴリズム X_A 、 X_B 、…により、その通信相手側との暗号通信用の共通鍵を生成する共通鍵生成手段6と、該共通鍵生成手段6により生成される共通鍵や前記乱数生成手段5により生成される乱数を鍵として、所謂、鍵共有方式による通信データの暗号化・復号化を行う暗号・復号手段7と、通信データの送信及び受信を行う暗号手段8と、後述の契約のための各種データの生成等の処理を担う契約処理システム9（詳細は後述する）とが備えられている。

【0046】この場合、暗号・復号手段7は、例えば3段のDES(Data Encryption Standard)により構成され、通信手段8は、モデムや通信処理用のソフトウェアにより構成されている。

【0047】また、乱数生成手段5は、一回性の数を種として、前記暗号・復号手段7に対する鍵として使用可能な乱数を生成するものである。具体的には、該乱数生成手段5により乱数を生成するに際しては、例えば端末装置1のユーザーにより、ある語句もしくは文章等が指示しないキーボードから端末装置1に入力され、このとき、乱数生成手段5は、その入力操作のタイミング（例えば各単語の入力時刻や各単語の入力の時間間隔）を計測する。この入力操作のタイミングの計測値は、あいまいさを有する人為的な入力操作に基づくため、偶然的で再現性のない一回性の数に相当するものとなる。そして、乱数生成手段5は、その入力操作のタイミングの計測値を種として、該計測値を前記暗号・復号手段7の暗号化・復号化のための鍵として使用可能なデータに変換することで、乱数を生成する。この場合、前記計測値を乱数に変換するに際しては、例えばハッシュ関数等の一方方向性関数による変換を行うことで、その変換結果として得られた乱数からその種である前記計測値を逆算することができないものとされる。このようにして乱数生成手段5により生成する乱数は、各ユーザーA、B、…同士の後述の契約に際して、その契約の受諾側当事者となるユーザー側の端末装置1において、該受諾側当事者に固有で、契約の申込み側当事者には予想のつかない受諾側固有データととして生成されるものである。

【0048】以上のような構成を有する本実施形態のシステムでは、例えばユーザーAがユーザーBから商品を購入したり、サービスの提供を受けるための契約等、ユ

ユーザーAを契約の申込み側当事者、ユーザーBを契約の受諾側当事者とした契約を両者間で締結する場合に、その契約は次のように行われる。

【0049】すなわち、図3を参照して、まず、契約の申込み側当事者であるユーザーAは、自身の端末装置1aにおいて、契約の受諾側当事者であるユーザーBの識別子を入力し、そのユーザーBの識別子と前記共通鍵生成用アルゴリズムX₁とから前記共通鍵生成手段6により、ユーザーBとの共通鍵K_{1a}を生成する(STEP1a)。

【0050】次いで、ユーザーBと締結しようとする契約内容(これはユーザーAが端末装置1a上で別途作成しておく)を、端末装置1aの暗号・復号手段7により、STEP1aで生成した共通鍵K_{1a}を用いて暗号化し、その暗号化した契約内容を通信手段8を介してユーザーBの端末装置1bに送信する(STEP2a)。これにより、ユーザーAは、ユーザーBに対して、契約の締結の意思表示を行う。

【0051】尚、この意思表示のために暗号化して送信する内容は、ユーザーAが最終的にユーザーBと締結しようとする契約内容そのものでなくてもよく、該契約内容の概要(骨子)を表した予備的な内容のものであってもよい。

【0052】一方、上記の送信を受けたユーザーBは、自身の端末装置1bにおいて、ユーザーAの識別子を入力し、そのユーザーAの識別子と前記共通鍵生成用アルゴリズムX₁とから前記共通鍵生成手段6により、ユーザーAとの共通鍵K_{1a}を生成する(STEP1b)。

【0053】次いで、ユーザーBは、前記乱数生成手段5によって、前述の如く該ユーザーBの端末装置1bへの入力操作のタイミングに基づく一回性の数(入力操作のタイミングの計測値)を種とした乱数を受諾側固有データとして生成する(STEP2b)。

【0054】そして、ユーザーBは、端末装置1bの暗号・復号手段7により、STEP2bで生成した乱数を、STEP1bで生成した共通鍵K_{1a}を用いて暗号化し、その暗号化した乱数を通信手段8を介してユーザーAの端末装置1aに送信する(STEP3b)。

【0055】この暗号化された乱数を受信したユーザーAは、その暗号化された乱数を受信した自身の端末装置1aの暗号・復号手段7によって、前記STEP1aで生成した共通鍵K_{1a}を用いて復号化する(STEP3a)。

【0056】また、ユーザーAは、自身の端末装置1aの前記契約処理システム9により、ユーザーAと締結しようとする契約内容と該ユーザーAとに固有の認証データを生成する(STEP4a)。すなわち、契約処理システム9は、ユーザーAの前記秘密鍵K_{1a}をパラメータとして決定される方向性関数としてのハッシュ関数を有しており、認証データの生成指示がユーザーAから与えられたとき、このハッシュ関数により契約内容を変換

することで、認証データ(ハッシュ値)を生成する。このように生成される認証データは、契約内容を、ユーザーAの秘密鍵K_{1a}により定まるハッシュ関数によって変換したものであるため、契約内容とユーザーAとに固有のものとなる。

【0057】次いで、ユーザーAは、このようにして生成した認証データとその元文である契約内容とを一括したものを、端末装置1aの暗号・復号手段7によって、前記STEP3aで復号した乱数(受諾側固有データ)を鍵として暗号化し、その暗号化した認証データ及び契約内容をユーザーBの端末装置1bに送信する(STEP5a)。これによりユーザーAはユーザーBに契約を申し込む。

【0058】上記のように暗号化された認証データ及び契約内容を受信したユーザーBは、その暗号化された認証データ及び契約内容を、端末装置1bの暗号・復号手段7によって、前記STEP3bで生成した乱数を鍵として復号化することで、暗号化されていない本来の認証データ及び契約内容を取得する(STEP5b)。さらに、ユーザーBはSTEP5bで取得した契約内容と、前記STEP2bで取得した契約内容とを照合し(STEP6b)、それらの内容の整合を確認した上で、ユーザーAから前述の如く申し込まれた契約を受諾し(STEP7b)、これによりユーザーA、B間の契約が成立する。

【0059】尚、ユーザーAは、前記STEP3aで復号化した乱数や、STEP5aで暗号化する前記認証データ及び契約内容を保管しておき、ユーザーBは、STEP3bで生成した乱数もしくはこの乱数の種とした一回性の数や、STEP5bで復号化した認証データ及び契約内容を保管しておく。このような実施形態の電子契約によれば、ユーザーBは、ユーザーAから契約の意思表示を受けたとき、ユーザーBに固有で、しかもユーザーAには判らない一回性の数を種として生成した乱数をユーザーAに与え、この乱数を鍵として暗号化された契約内容をユーザーAから受け取るため、ユーザーBは、自身が独自にユーザーAに対して指定した該ユーザーAに固有の方式で、ユーザーAから前記契約内容に従った契約の申込みを受けることとなる。

【0060】このため、ユーザーBにとっては、ユーザーAによる契約の締結の意思が明確なものとなる。同時に、ユーザーAはユーザーBにより指定された独特の方式でユーザーBに契約を申し込むこととなるため、契約事実を事後否定しにくくなる。従って、ユーザーBにとって、ユーザーAから申し込まれた契約の信頼性が高まる。

【0061】さらに、ユーザーAは、ユーザーBに最初に契約の締結の意思表示をするに際して、ユーザーBと締結しようとする契約内容あるいはその概要(骨子)をユーザーBに与えておくため、ユーザーBは、最終的に

ユーザーAとの契約を受諾するに際して、最初に受け取った契約内容もしくはその概要(STEP2bで復号化したもの)と、最終的に受け取った契約内容(STEP5bで復号化したもの)とを照合して両者の矛盾の有無を確認した上で、ユーザーAとの契約を受諾することができ、これによっても、ユーザーAとの契約の信頼性が高まる。

【0062】また、ユーザーAは、自身に固有の秘密鍵 K_{SA} によって定まるハッシュ関数(一方方向性関数)によって、契約内容を変換してなる認証データをユーザーBに与えるため、ユーザーA、Bの両者にとっての契約の信頼性が一層強固なものとなる。

【0063】すなわち、前記認証データは、ユーザーAに固有の秘密鍵 K_{SA} によって定まるハッシュ関数(一方方向性関数)によって、契約内容を変換したものであるため、ユーザーAと契約内容に固有で、しかも、ユーザーBには生成することができないものである。そして、ユーザーAの秘密鍵 K_{SA} は、ユーザーA、Bの両者から中立的な立場にある前記公証人Sが必要に応じて認証可能なものである。このため、前記認証データをユーザーAからユーザーBに与えるということは、ユーザーAが、ユーザーBと締結する契約内容に公的な署名もしくは捺印を施したものをユーザーBに与えるということの意味する。

【0064】この場合、ユーザーBは、ユーザーAから認証データを受け取った時点では、その認証データが適正なものであるか否かは判らないものの、必要に応じて公証人Sによって、ユーザーBあるいはユーザーAが保管している契約内容をユーザーAの秘密鍵 K_{SA} により定まるハッシュ関数で変換してもらい、それをユーザーAからユーザーBに与えられた認証データと照合することによって、ユーザーAからユーザーBに与えられた認証データの真偽を証明してもらうことができる。

【0065】また、ユーザーBは、認証データに反映されるユーザーAの秘密鍵 K_{SA} を知らないため、仮にユーザーBがユーザーAとの契約の締結後に、ユーザーAから受け取った契約内容を改ざんしようとしても、その改ざんした契約内容と整合するような認証データを生成することはできず、その結果、ユーザーBによる契約内容の改ざんができない。

【0066】さらに、前記認証データは契約内容を一方方向性関数としてのハッシュ関数により変換したものであるため、仮に、契約後にユーザーAが契約内容を改ざんしようとしても、ユーザーBに与えた認証データと整合するようにユーザーAが契約内容を改ざんすることも困難である。

【0067】従って、前述のような認証データをユーザーAからユーザーBに与えることで、該ユーザーA、Bの両者にとって、契約の信頼性が強固なものとなる。

【0068】また、契約に際しての両ユーザーA、B間

の通信は、共通鍵 K_{AB} あるいは乱数を鍵とした暗号通信によって行われるため、契約内容や認証データの部外者に対する機密性が確保される。この場合、前記乱数の暗号通信のための前記共通鍵 K_{AB} は、各ユーザーA、Bが自身の端末装置1a、1bの共通鍵生成手段6に相手側の識別子を入力するだけで鍵管理系C等の関与を要することなく、生成することができ、また、最終的な契約内容や認証データの暗号通信を行うための鍵として使用する乱数は、ユーザーBが自身の端末装置1bの乱数生成手段5により生成し、それを共通鍵 K_{AB} により暗号化してユーザーAの端末装置1aに送信するだけで、ユーザーA、Bの両者で共有することができる。

【0069】従って、両ユーザーA、Bは、契約のための通信を簡単に行うことができる。また、鍵管理系Cは、各ユーザーA、B、…に共通鍵生成用アルゴリズムや秘密鍵 K_{SA} 、 K_{AB} 、…を配付した後は、公開鍵方式の場合のような鍵の保守・管理等を行う必要がないため、該鍵管理系Cの負担は小さい。

【0070】このため、本実施形態の電子契約を行うシステムを簡易で普及性の高いものとすることができる。

【0071】次に本発明の第2の実施形態を図4を参照して説明する。尚、本実施形態は、前記第1の実施形態のものと、システム構成は同一であるので、構成部分については、図1及び図2の参照符号を用いて説明を省略する。

【0072】図4を参照して、本実施形態では、二人のユーザーA、B間で、前記第1の実施形態と同様の契約を締結する場合、該第1の実施形態と全く同様、ユーザーAからユーザーBへの契約の締結の意思表示と、これに続くユーザーBからユーザーAへの乱数(受諾側固有データ)の受け渡しとが行われる(ユーザーA側のSTEP1a～STEP3a及びユーザーB側のSTEP1b～STEP3b)。

【0073】一方、ユーザーBから乱数を受け取ったユーザーAは、その端末装置1aの契約処理システム9により、ユーザーBと締結しようとする契約内容に固有で且つ該ユーザーAに固有の認証データを次のように生成する。

【0074】すなわち、ユーザーAの端末装置1aの契約処理システム9とユーザーBの端末装置1bの契約処理システム9とは同一のハッシュ関数(一方方向性関数)を有しており、ユーザーAの端末装置1aの契約処理システム9はユーザーAから認証データの生成指示が与えられたとき、ユーザーAがユーザーBと締結しようとする契約内容を、まず、上記ハッシュ関数により変換する(STEP4a)。

【0075】尚、上記のようなハッシュ関数は、あらかじめ全てのユーザーA、B、…について同一として設定しておいてもよいが、例えば、それらのユーザー同士が契約を締結する際に使用する共通鍵 K_{AB} 、…や乱数をバ

ラメータとして契約の都度、設定するようにしてもよい。

【0076】次いで、ユーザーAの契約処理システム9は、STEP4aの変換により得られた変換データ（ハッシュ値）を、前記暗号・復号手段7によって、ユーザーAの秘密鍵K_sにより暗号化せしめることで、認証データを生成する（STEP6a）。この場合、前記変換データをユーザーAの秘密鍵K_sにより暗号化して認証データを生成することで、該認証データは契約内容とユーザーAとに固有のものとなる。

【0077】このようにして、認証データを生成した後、ユーザーAは、その認証データと、該認証データを生成する過程で得られた変換データと、これらの元文である契約内容とを、STEP3aで復号化して得た乱数を鍵として、暗号・復号手段7により暗号化し、その暗号化した認証データ、変換データ及び契約内容をユーザーBの端末装置1bに送信する（STEP5a）。

【0078】また、暗号化された認証データ、変換データ及び契約内容を受信したユーザーBは、その暗号化された認証データ、変換データ及び契約内容を、それぞれSTEP3bで生成した乱数を鍵として、暗号・復号手段7により復号化することで、暗号化されていない本来の認証データ、変換データ及び契約内容を取得する（STEP5b）。そして、ユーザーBはSTEP5bで取得した契約内容と、前記STEP2bで取得した契約内容とを照合し（STEP6b）、それらの内容の整合を確認する。

【0079】さらに、ユーザーBは、自身の端末装置1bの契約処理システム9によって、STEP5bで取得した契約内容をユーザーA側と同一のハッシュ関数により変換し（STEP7b）、その変換により得られたデータと、STEP5bで取得した変換データとを照合し（STEP8b）、両者のデータが一致しているか否かを確認する。

【0080】そして、STEP6bで契約内容の整合性が確認され、且つSTEP8bで変換データの一致が確認されると、ユーザーBはユーザーAから与えられた契約内容に従ってユーザーBとの契約を受諾する（STEP9b）。

【0081】尚、ユーザーAは、前記STEP3aで復号化した乱数や、STEP5aで暗号化する前の認証データ、変換データ及び契約内容を保管しておき、ユーザーBは、STEP3bで生成した乱数もしくはこの乱数の種とした一回性の数や、STEP5bで復号化した認証データ、変換データ及び契約内容を保管しておく。

【0082】このような本実施形態の電子契約によれば、ユーザーBからユーザーAへの乱数の受け渡しや、ユーザーAからユーザーBへの認証データの受け渡し等によって、前記第1の実施形態と同様の作用効果を奏することができる。

【0083】さらに本実施形態では、ユーザーA側で認証データを生成する際に、契約内容をユーザーB側と同じハッシュ関数により変換してなる変換データをユーザーAからユーザーBに与え、ユーザーB側で、その変換データを確認することで、契約の信頼性をさらに高めることができる。すなわち、ユーザーB側で、ユーザーAから送られてきた契約内容をハッシュ関数により変換してなるデータと、ユーザーAから送られてきた変換データとが一致するということは、ユーザーAが変換データを生成し、さらには認証データを生成する際の元文とした内容と、ユーザーAがユーザーBに送った契約内容とが一致すること意味する。従って、ユーザーB側で、ユーザーAから送られてきた契約内容をハッシュ関数により変換してなるデータと、ユーザーAから送られてきた変換データとを照合して、それらの一致を確認することで、ユーザーB側では、ユーザーAが認証データを生成するに際して、正しい契約内容からハッシュ関数により変換データを生成したか否かを確認することができ、これにより、契約の信頼性をより一層高めることができる。

【0084】次に、本発明の第3の実施形態を図5を参照して説明する。尚、本実施形態は、前記第1及び第2の実施形態のものと、システム構成は同一であるので、構成部分については、図1及び図2の参照符号を用いて説明を省略する。

【0085】図5を参照して、本実施形態では、二人のユーザーA、B間で、前記第1及び第2の実施形態と同様の契約を締結する場合、該第1及び第2の実施形態と全く同様に、ユーザーAからユーザーBへの契約の締結の意思表示と、これに続くユーザーBからユーザーAへの乱数（受話側固有データ）の受け渡しとが行われる（ユーザーA側のSTEP1a～STEP3a及びユーザーB側のSTEP1b～STEP3b）。

【0086】一方、ユーザーBから乱数を受け取ったユーザーAは、その端末装置1aの契約処理システム9により、ユーザーBと締結しようとする契約内容に固有で且つ該ユーザーAに固有の認証データを次のように生成する。

【0087】すなわち、ユーザーAは、ユーザーBへの契約の申込みの日時を、前記第2の実施形態と同様にユーザーB側と同一のハッシュ関数を有する前記契約処理システム9に入力し、該契約処理システム9のハッシュ関数によって契約の申込みの日時を変換して成るタイムスタンプ（契約の申込みの日時に応じたデータ）を生成する（STEP4a）。

【0088】そして、ユーザーAは、STEP4aで生成したタイムスタンプと、ユーザーBと締結する契約内容とを合わせたものを、契約処理システム9のハッシュ関数によって変換して、変換データ（ハッシュ値）を生成し（STEP5a）、さらにその変換データを前記第2

の実施形態と同様に、ユーザーAの秘密鍵 $K_{A,a}$ により暗号化することで認証データを生成する(STEP 7a)。

【0089】次いで、ユーザーAは、契約内容と、タイムスタンプと、交換データと、認証データとを、STEP 3aで復号化して得た乱数を鍵として、暗号・復号手段7により暗号化し、その暗号化した契約内容、タイムスタンプ、交換データ及び認証データをユーザーBの端末装置1bに送信する(STEP 6a)。

【0090】また、暗号化された契約内容、タイムスタンプ、交換データ及び認証データを受信したユーザーBは、その暗号化された契約内容、タイムスタンプ、交換データ及び認証データを、それぞれSTEP 3bで生成した乱数を鍵として、暗号・復号手段7により復号化すること、暗号化されていない本来の契約内容、タイムスタンプ、交換データ及び認証データを取得する(STEP 5b)。そして、ユーザーBはSTEP 5bで取得した契約内容と、前記STEP 2bで取得した契約内容とを照合し(STEP 6b)、それらの内容の整合を確認する。

【0091】さらに、ユーザーBは、自身の端末装置1bの契約処理システム9によって、STEP 5bで取得した契約内容とタイムスタンプとを合わせたものをユーザーA側と同一のハッシュ関数により変換し(STEP 7b)、その変換により得られたデータと、STEP 5bで取得した交換データとを照合し(STEP 8b)、両者のデータが一致しているか否かを確認する。

【0092】そして、前記第2の実施形態と同様に、STEP 6bで契約内容の整合性が確認され、且つSTEP 8bで交換データの一致が確認されると、ユーザーBはユーザーAから与えられた契約内容に従ってユーザーBとの契約を受諾する(STEP 9b)。

【0093】尚、ユーザーAは、前記STEP 3aで復号化した乱数や、STEP 5aで暗号化する前の認証データ、交換データ及び契約内容と、タイムスタンプもしくは該タイムスタンプの元とした契約の申込みの日時とを保管しておき、ユーザーBは、STEP 3bで生成した乱数もしくはこの乱数の種としたり一回性の数や、STEP 5bで復号化した認証データ、交換データ、契約内容及びタイムスタンプを保管しておく。

【0094】さらに、本実施形態では、ユーザーA及びBは、上記のように保管するデータを公証人Sに送って保管せしめる。この場合、各ユーザーA、Bが公証人Sにデータを送るに際しては、それぞれ、公証人Sとの共通鍵 $K_{S,a}$ 、 $K_{S,b}$ (=各ユーザーA、Bの秘密鍵)を使用した暗号通信によって、データを公証人Sに送る。

【0095】このような本実施形態の電子契約によれば、ユーザーBからユーザーAへの乱数の受け渡しや、ユーザーAからユーザーBへの認証データの受け渡し等によって、前記第1の実施形態と同様の作用効果を奏す

ることができる。さらに、前記第2の実施形態と同様に、ユーザーB側で、交換データの確認を行うことで、契約の信頼性を高めることができる。

【0096】また、本実施形態では、交換データや認証データには、契約内容に加えて、ユーザーAによる契約の申込みの日時が反映されるため、これらのデータは契約内容のみならず、ユーザーAによる契約の申込みの日時にも固有のものとなり、それらのデータに基づく契約の信頼性がより強固なものとなる。特に、本実施形態では、契約の申込みの日時をそのまま使用して、交換データや認証データを生成するのではなく、該日時をハッシュ関数により変換した上で、それを交換データや認証データに反映させるため、例えばユーザーAがユーザーBに送ったタイムスタンプと整合するように契約の申込みの日時を偽ったりすることが困難であり、その結果、そのタイムスタンプがユーザーAによる契約の申込みの日時を確定する上で有効なものとなる。

【0097】さらに、本実施形態では、各ユーザーA、Bは、契約内容はもちろん、前記乱数もしくはその種である一回性の数、認証データ、交換データ、並びに、タイムスタンプもしくはその元となる契約の申込みの日時を公証人Sに送って保管せしめるので、ユーザーA、B間の契約の事実を確実なものとしてすることができる。

【0098】尚、以上説明した各実施形態では、ユーザーA側で交換データや認証データを生成する際に、契約内容そのものを使用するようにしたが、該契約内容をユーザーBから与えられた乱数を鍵として暗号化したものから、交換データや認証データを生成するようにしてもよい。このようにした場合には、前記交換データや認証データには、契約内容やユーザーAに固有の秘密鍵 $K_{A,a}$ だけでなく、ユーザーBが生成したユーザーBに固有の乱数も反映されるため、それらの交換データや認証データに基づく契約の効力を両ユーザーA、Bにとって、より強固なものとすることができる。

【0099】また、前記第1及び第2の実施形態では、各ユーザーA、Bが乱数もしくはその種である一回性の数や、認証データ等を前記第3の実施形態と同様に、公証人Sに送って保管せしめるようにしてもよい。

【0100】また、前記各実施形態では、認証データを生成するための秘密鍵 $K_{A,a}$ として、公証人Sとの共通鍵を使用するようにしたが、公証人Sとは無関係に各ユーザー毎に固有の秘密鍵を鍵管理局Cで生成して各ユーザーに配付しておくようにすることも可能である。但し、この場合には、公証人Sは、各ユーザーの秘密鍵を認証するためには、各ユーザーの秘密鍵を保管しておかなければならず、公証人Sの負担が大い。これに対して、前記各実施形態のように、各ユーザーの秘密鍵として公証人Sの共通鍵を使用することで、公証人Sは自身が所持する共通鍵生成用アルゴリズムに各ユーザーの識別子

を入力することで、随時、各ユーザーの秘密鍵を生成することができ、該公証人Sの負担が極めて小さくて済む。

【0101】また、前記各実施形態では、受諾側固有データとして乱数を用いたが、例えば受諾側当事者（ユーザーB）の端末装置1bにおける入力操作の時刻を受諾側固有データとして用い、その時刻から申込み側当事者（ユーザーA）がデータの改ざんをできないような時間内で、該申込み側当事者に受諾側当事者への契約の申込みを行わせるようにしてもよい。

【図面の簡単な説明】

【図1】本発明の第1の実施形態を適用した電子契約システムの全体の構成を示す説明図。

【図2】本発明の第1の実施形態において契約を行う当

* 事者が所持する端末装置の機能的構成を示すブロック図。

【図3】本発明の第1の実施形態で契約を行う際の処理手順を示すフロー図。

【図4】本発明の第2の実施形態で契約を行う際の処理手順を示すフロー図。

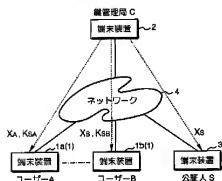
【図5】本発明の第3の実施形態で契約を行う際の処理手順を示すフロー図。

【符号の説明】

- 10 1(1a, 1b, ...)…端末装置、A, B…ユーザー（契約の当事者）、S…公証人（第三者）、 K_{iA} …共通鍵、 K_{iA} …秘密鍵、5…乱数生成手段、6…共通鍵生成手段、7…暗号・復号手段。

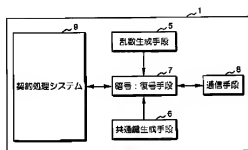
【図1】

FIG. 1

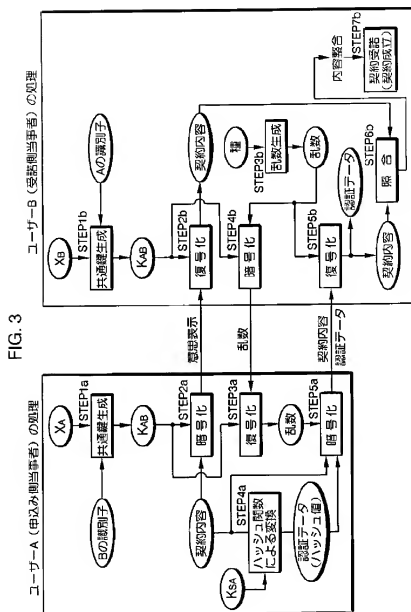


【図2】

FIG. 2



【図3】



【図4】

